IT Radix Resource

We make IT Work for You

October 2019

Traditions and Technology

Corn Mazes: Finding Your Way Out!

Mazes and labyrinth-like structures have fascinated us since ancient times. The modern-day version is what we know today as a corn maze. Visiting a corn maze has become a popular fall tradition and has helped the entrepreneurial farmer find a way to generate extra income from tourists. Wikipedia reports that the first corn maze built in America was created by Don Frantz and Adrian Fischer in Annville, Pennsylvania, just over two hours away from IT Radix. That was in 1993 and the maze covered 3 acres with just under two miles of paths. Mazes have grown bigger and more popular ever since. According to the Guinness Book of World Records, the largest corn maze in the United States was reportedly created by Cool Patch Pumpkins in Dixon, California, in 2014. It covered over 60 acres, that is quite literally a big enterprise!

And like any big enterprise, a lot of planning really needs to go into creating a successful corn maze. A maze really is a network of paths, openings and dead ends! And creating a network track is much like creating an information technology network for a commercial enterprise.

> Relying on the experts for advice and support is the least expensive and most profitable decision in the long run.

The Big Picture – In early network architecture planning, the goal was just connecting a few computers, so staff could communicate and share—just get from point A to point B with their data, like walking through that first corn maze in Annville. But things have progressed a great deal since then. Today, to plan a corn maze, the planners start with the big picture and by that we mean things like what image will the maze depict from above? When creating an information technology network today, the big picture is the place to start as well. What is the goal? What is the vision? What values in terms of productivity and security will this network deliver?

The Grid – A corn maze design is only as good as the job spent cutting it. The cuts need to be precise and need to lead to the correct destinations, whether to the focal point of the maze design or to the way out! Also access into the maze and egress out of the maze must be well planned and secure. There are dozens of companies today whose sole purpose is corn maze design. Amazingly, today's larger, more entrepreneurial farmers rely on outside resources to help them plan, create and manage their mazes. They know that relying on the experts for advice and support is the least expensive and most profitable decision in the long run. Sounds a lot like planning a computer network and deciding which network machines and users can get into the network and access files easily and securely. The smart business person relies on a resource like IT Radix to facilitate all of this in planning—even more importantly, in execution.

(Continued on page 2)

What's New

October is National Cyber Security Awareness Month

Ask us about our Security Awareness training in honor of National Cyber Security Awareness Month.

October 6

100 Day Countdown

Windows 7 and Windows Server 2008 will reach their end of life on January 14, 2020. No time like the present to makes plans to migrate to Windows 10 before it's too late.

October 24

Webinar

10-Minute Tech Talk:

* Tech Tales from the Crypt *

How to Avoid Becoming

One of Them

www.it-radix.com/webinar

Starts @12:10 sharp

If you would rather receive our newsletter via email, sign up on our website or send an email to resource@it-radix.com

More free tech tips at:
www.it-radix.com/blog

When Mischief Night Becomes a Nightmare

Mischief Night, the day before Halloween, is a celebration where the revelers engage in harmless pranks; however, in the business world, your staff can create much more than harmless mischief if they are not properly trained and following IT security procedures.

For example, most people do not intentionally give away their email passwords; however, often they are not properly trained to recognize a phishing email or the organization doesn't enforce multi-factor authentication because it's not convenient. We recently learned of an organization that fell victim to a combination of a phishing campaign as well as a look-alike domain name and lost $660,000 dollars as a result. Clearly, cyber criminals aren't just looking to make mischief; the potential financial booty is tremendous. So, what do you do to avoid turning Mischief Night into *Nightmare on Elm Street*?

Train your employees on IT security! We cannot say it enough. Every organization needs to train their employees on an ongoing basis to ensure they understand your security policy and recognize potential risks. Encourage a "neighborhood watch" approach. If someone notices anything suspicious, such as not being able to log into an email account right away, have them notify your IT staff immediately.

IT Radix offers both online security awareness training as well as ongoing testing to ensure your team is actually learning and applying the training to real-world emails. We also have an email IT Security Tips series that we encourage you to share with your team. IT security training is not a one-and-done process. Every organization needs to constantly reinforce security and appropriate training.

Use strong passwords and secure any shared passwords. It goes without saying that everyone should create strong, complex passwords. Additionally, you should avoid reusing the same password string in multiple systems. The average person must keep track of 90-120 accounts and passwords. As a result, IT Radix now recommends the use of a password manager that not only tracks passwords but also audits and reports on who is using these passwords within an organization. We offer a business-class password management system to all our clients.

Enforce multi-factor authentication. Yes, it might take one more step to login, but the increased security benefits far outweigh this minor inconvenience. Multi-factor authentication requires a basic password along with a second piece of information or an actual device (such as your smartphone) to login to critical systems such as email, your accounting system or line-of-business application.

Through training and strong security practices, your organization can keep the fun in Mischief Night and the nightmares out of your business.

Welcome!

A warm welcome to our newest **Management and Support** clients:

C3Workplace
Frederic's Fine Jewelers
IBN Diamond Corporation

Remember, IT Radix is here to service all of your technology needs!

Corn Mazes: Finding a Way Out!

(Continued from page 1)

The Operation – After all the planning, planting, cutting and promoting is done, it is time for the farmer to invite in the public and turn the amazing network into an attraction that delivers him or her real value…real money. And that is done with the operation of the maze, adding in games, rides and contests. Some mazes are kid friendly all day long…and haunted at night! Just like maximizing the value of a corn maze, business and organization leaders today rely on outside services such as backup systems, antivirus and other security services to make things run smoothly!

Contact IT Radix today and let us help you navigate your technology maze and make IT work for you!

OUR CLIENTS SPEAK OUT:

THE BUZZ

"IT Radix has been an invaluable partner supporting SPI Group and offering innovative ideas for how we can reinforce and expand our infrastructure. From dealing with the simplest of tasks to handling the most complex requests, everyone at IT Radix has been extremely helpful and knowledgeable."

Tom Gilbert, Director Interactive & Infrastructure — SPI Group, LLC

SPI Group is an award-winning agency that uses digital solutions to amplify employee communications. They do their best work where communications and innovative technologies overlap. Their integrated services cut across strategy, design, editorial and web development.

Let's Get Carving!

Leaves are falling and Halloween is right around the corner. Eager pumpkin carvers are preparing orange masterpieces to decorate their porches, but did you know the jack-o'-lantern once served an entirely different purpose?

The ancient tradition of the jack-o'-lantern was once believed to ward off unwanted spirits, scaring off monsters that might otherwise go bump in the night. Interesting fact, what does it have to do with my IT?

This October, instead of a jack-o'-lantern, consider placing an enhanced network security solution like Open DNS on your company's front porch to help protect your network from goblins. Open DNS scans network traffic for hidden or malicious content, blocking or intercepting unseen dangers that may have otherwise compromised a user's information or machine!

Would you like to secure your network and carve out your own network jack-o'-lantern? Give us a call, and let's get carving!

Proudly folded & stuffed by Central Park School

SPECIAL OFFER

Online Shopping

Keep track of your online shopping accounts more easily this holiday season. Sign up for a year of IT Radix Passport during the months of **October**, **November** and **December**, and get a *Baker's Dozen*—that's 13 months for the price of 12.

Visit IT Radix at www.it-radix.com to learn more about our services.

Masquerading to Attack Your Network

Many of us enjoy Halloween and have a lot of fun dressing up and pretending to be someone or something we are not. Who doesn't love a masquerade party? However, when it comes to your company's network, a visitor in disguise is not welcome.

Most small and midsize business (SMB) owners focus on the day-to-day operations of their organization, driving growth, facilitating hiring and guiding marketing, without a single thought to the security of the computer networks these processes depend on. Unfortunately, according to Verizon's annual Data Breach Investigations Report, a full 71% of cyberattacks are aimed squarely at SMBs that are known to have less secure networks than larger companies. How do hackers infiltrate hapless small businesses?

Phishing Emails

An employee receives an email directly from your company's billing company, urging them to fill out some "required" information before their paycheck can be finalized. Included in the very professional looking email is a link your employee needs to click to complete the process. But when they click the link, a host of vicious malware floods their system, spreading to the entirety of your business network within seconds, and locks everyone out of their most precious data. In return, the hackers want thousands of dollars, or they'll delete everything. Today it's easier than ever for an attacker to gather information and make a phishing email look like every other run-of-the-mill email you receive each day. Train your employees to recognize these sneaky tactics and put safeguards in place in case someone clicks the malicious link.

Bad Passwords

According to Inc.com contributing editor John Brandon, "With a $300 graphics card, a hacker can run 420 billion simple, lowercase, eight-character password combinations a minute." What's more, he says, "80% of cyberattacks involve weak passwords," yet despite this fact, "55% of people use one password for all logins." There's simply no excuse for using an easy-to-crack password. Instead, it's good practice to make a password out of four random common words, splicing in a few special characters for good measure. HowSecureIsMyPassword.net will check the strength of your password.

Malware

While malware is often delivered through a shady phishing email, that's not the only way it can wreak havoc on your system. An infected website (such as those you visit when you misspell sites, a technique called "typosquatting"), a USB drive loaded with viruses or even an application can invite vicious software into your world. These days, antivirus software is not enough—you need a combination of software systems to combat these threats.

Social Engineering

As fallible as computers may be, they've got nothing on people. Sometimes hackers don't need to touch a keyboard at all to break through your defenses—they can simply masquerade as you in order to get a team member to activate a password reset. It's easier than you think and requires carefully watching what information you put on the Internet. Don't put the answers to your security questions out there for all to see.

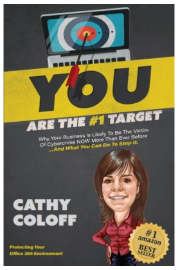
The best way to protect yourself from masked intruders is to partner with an IT expert that constantly keeps your system updated with cutting-edge security. Let IT Radix help you unmask any uninvited guests and protect your network.

"Tradition is a very powerful force."

— John P. Kotter, Educator

"You must pinky-swear to never reveal our company secrets. That's the cornerstone of our new information security program."

From the desk of: Cathy Coloff
Subject: You are the #1 Target!



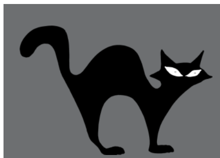
Generally, everyone fears something. Halloween is one of those traditions that pokes fun at, while at the same time plays off of, people's fears. As I've grown older, my childhood fears of things that go bump in the night have disappeared and been replaced by other fears that perhaps I have yet to discover. Something I have not had a fear of is writing. I've always enjoyed writing and so, when I was approached to contribute to a cyber book, I happily agreed.

The book is a compilation of articles from a number of my industry colleagues and experts on a variety of cybersecurity topics. Given that so many of our clients are using Office 365, I decided to focus my chapter of the book on some basic security tips and techniques for this service. I'm proud to say the book is finally complete and was launched on Amazon on September 12th. If you'd like a copy of the book or just my chapter, I'd be more than happy to share. Many authors will say writing a book (or a chapter, in my case) is a labor of love and now, having done it, I agree. My hope is that a business owner will apply even just one of the ideas in the book to their business to increase its cybersecurity posture.

Having now been through the book-writing process, the jury is still out as to whether I'd do it again. Perhaps a memoir of IT horror stories in honor of Halloween might be interesting and fun. In the meantime, I plan to simply enjoy the upcoming Halloween holiday with some fun decorations, a silly costume and, of course, candy!

Cathy

Happy Halloween everyone!



Enter and Win Trivia Contest

The first person to send an email to resource@it-radix.com with the correct answer to our trivia question will win an Amazon gift card.

Q: What popular fall festival activity did the Romans bring to Britain when they invaded?

July Trivia Challenge

Q: What is the name of the trophy awarded to the winner of the America's Cup sailing race?

(Answer: Auld Mug)

Congratulations to Colette Abramo of Jansons Associates, recipient of an REI gift card.

Candy Apples: Layered to Perfection

Who doesn't love a bright red candy apple! In 1908, William W. Kolb, a candy-maker from Newark, New Jersey, is said to have invented the red candy apple. As the story goes, Kolb was experimenting and dipped some apples in a red cinnamon candy mixture—selling them for 5 cents each. Soon, candy apples were sold at the Jersey shore and later at circuses and candy shops nationwide.

Caramel apples were also the result of an experiment. In the 1950s, a Kraft Foods employee, Dan Walker, is credited for inventing them. With a surplus of caramels left over from Halloween sales, Walker experimented with dipping apples into the melted caramels—and the rest is history. While caramel apples were made by hand for the first decade of their existence, Vito Raimondi of Chicago, Illinois, made and patented the first automated caramel apple machine in 1960.

And, anyone who has visited a theme park in the past 20+ years can vouch that candy apples have turned into a gourmet treat—dipped in layers and layers of caramel, chocolate, and sprinkled with all sorts of confections.

Does your network have layers to protect itself from hackers? A layered approach to security is essential. Layers like proactive maintenance, policy-driven protection, patch management, encryption, and two-factor authentication are just a few layers that should be implemented. They will not prevent an attack, but will certainly slow down an intruder and buy you some time

Don't break a tooth or lose a filling while enjoying a sweet confection. Let IT Radix provide recommendations to help improve your network protection.